(51) Int. Cl. 2: H 04 L 9/02

(19) BUNDESREPUBLIK DEUTSCHLAND
DEUTSCHES PATENTAMT

3

DE 27 06 421 B 1

(11) Auslegeschrift 27 06 421

(21) Aktenzeichen: P 27 06 421.7-31
(22) Anmeldetag: 16. 2. 77
(43) Offenlegungstag: —
(44) Bekanntmachungstag: 29. 6. 78

(30) Unionspriorität:
(32) (33) (31) —

(54) Bezeichnung: Verfahren zum Einstellen von Schlüsseltextgeneratoren in Chiffriergeräten

(71) Anmelder: Licentia Patent-Verwaltungs-GmbH, 6000 Frankfurt

(72) Erfinder: Glitz, Ekkehard, Ing.(grad.), 7150 Backnang

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE-AS 12 37 366
DE-OS 24 57 027

DE 27 06 421 B 1

6. 78 809 526/513

Patentansprüche:

1. Verfahren zur Ver- und Entschlüsselung der Datenübertragung zwischen einem Sender und mindestens einem Empfänger, bei welchem sendeseitig die Nachrichtenklartexte mit Schlüsseltexten verknüpft und empfangsseitig durch Verknüpfung mit identischen Schlüsseltexten wiedergewonnen werden und bei welchem sende- und empfangsseitig derselbe Grundschlüssel in gespeicherter Form vorliegt, dadurch gekennzeichnet, daß vor der Nachrichtenübertragung folgende Verfahrensschritte angewendet werden:

a) vor Beginn der Nachrichtenübertragung würfelt der sendeseitige Schlüsseltextgenerator mit Hilfe eines beliebigen und/oder eines während des Würfelns sich beliebig ändernden Bildungsgesetzes mindestens ein Schlüsseltextbildungsregister (*A*) eine gewisse Mindestzeit lang mit einem zum Übertragungstakt verschiedenen nichtperiodischen Durchlauftakt (*T1*), bis im Schlüsseltextbildungsregister (*A*) eine zufällige Bitfolge von *n* Elementen erreicht ist (Fig. 2),

b) diese zufällige Bitfolge wird festgehalten und dient als Anfangsstellung für die Schlüsseltextgeneratoren auf der Sende- und auf der Empfangsseite,

c) diese zufällige Bitfolge wird vor Beginn der Nachrichtenübertragung vom Sender zu dem/den Empfänger/n übertragen, wobei sendeseitig die Schlüsseltextbildungsregister (*A*) zyklisch so geschoben werden, daß nach der Übertragung die sende- und empfangsseitigen Schlüsseltextgeneratoren dieselbe Ausgangsstellung haben,

d) die Übertragung der Anfangsstellung der Schlüsseltextgeneratoren wird durch ein Kennwort angekündigt und unter Verwendung einer sende- und empfangsseitig bekannten gleichartigen Grundschlüsselinformation verschlüsselt übertragen,

e) das Bildungsgesetz der Schlüsseltextgeneratoren wird aus der sendeseitig erzeugten und verschlüsselt zu dem/den Empfänger/n übertragenen zufälligen Bitfolge abgeleitet, daß während der Nachrichtenübertragung bei wiederholender Synchronisation, wie dies bei Rundspruch notwendig ist, der Nachrichtenfluß kurzzeitig unterbrochen wird und folgende Verfahrensschritte angewendet werden:

f) die zum Zeitpunkt der Unterbrechung in den Schlüsseltextbildungsregistern (*A*) des Senders festgehaltene Bitfolge dient als Anfangsstellung der Schlüsseltextgeneratoren für neu hinzukommende Empfänger oder zur Überprüfung des Gleichstandes der zu einem früheren Zeitpunkt synchronisierten Empfänger,

g) diese zum Zeitpunkt der Unterbrechung sendeseitig festgehaltene Bitfolge der Schlüsseltextbildungsregister (*A*) wird durch ein Kennwort markiert und unter Verwendung einer sende- und empfangsseitig bekannten identischen Grundschlüsselinformation verschlüsselt übertragen,

h) das Bildungsgesetz der Schlüsseltextgeneratoren wird beibehalten oder aus der festgehaltenen Bitfolge der Schlüsseltextbildungsregister (*A*) sende- und empfangsseitig abgeleitet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Verschlüsselung der zu übertragenden Anfangsstellung für den Schlüsseltextgenerator mit Hilfe eines linear rückgekoppelten Schieberegisters erfolgt, dessen Voreinstellung und/oder Bildungsgesetz vom Grundschlüssel (*GS*) abhängt (Fig. 3).

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Verschlüsselung der zu übertragenden Anfangsstellung für den Schlüsseltextgenerator mit Hilfe des vom Grundschlüssel (*GS*) eingestellten Senders (Fig. 1) selbst erfolgt, daß die Anfangsstellung zuerst in einem Zwischenspeicher gespeichert wird, daß die Anfangsstellung nach der Entschlüsselung auf der Empfangsseite ebenfalls in einem Zwischenspeicher gespeichert wird und daß vor Beginn der eigentlichen Nachrichtenver- und -entschlüsselung die Anfangsstellung aus den Zwischenspeichern in die Schlüsseltextgeneratoren übernommen wird.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß ein erster Teil der die Anfangsstellung darstellenden Elemente sendeseitig erwürfelt wird und verschlüsselt zur Empfangsseite übertragen und eingestellt wird und ein zweiter Teil der die Anfangsstellung darstellenden Elemente sende- und empfangsseitig abhängig vom Grundschlüssel eingestellt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Bildungsgesetz sendeseitig im Schlüsseltextgenerator erwürfelt und zusätzlich zur Anfangsstellung des Schlüsseltextbildungsregisters (*A*) verschlüsselt zur Empfangsseite übertragen wird.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß das Bildungsgesetz des Schlüsseltextgenerators sende- und empfangsseitig nach Einstellung der Schlüsseltextbildungsregister (*A1* bis *An*) nach einer vereinbarten Vorschrift im Schlüsseltextgenerator errechnet und im Zwischenspeicher gespeichert wird und vor der eigentlichen Nachrichtenver- bzw. -entschlüsselung das errechnete Bildungsgesetz aus dem Zwischenspeicher in das jeweilige Bildungsgesetzregister (*B*) des Schlüsseltextgenerators übernommen wird.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der sendeseitige Würfelvorgang zum Erzeugen der zufälligen Anfangsstellung des Schlüsseltextgenerators mit Hilfe eines Zufallsgenerators gesteuert wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Anzahl *n* der die Anfangsstellung darstellenden Elemente $n \geqq 50$ gewählt wird.

Die Erfindung betrifft ein Verfahren zur Ver- und Entschlüsselung der Datenübertragung zwischen einem Sender und mindestens einem Empfänger, bei welchem sendeseitig die Nachrichtenklartexte mit

Schlüsseltexten verknüpft und empfangsseitig durch Verknüpfen mit identischen Schlüsseltexten wiedergewonnen werden und bei welchem sende- und empfangsseitig derselbe Grundschlüssel in gespeicherter Form vorliegt.

Die Erfindung dient nicht nur zur Datensicherung vor unberechtigtem Zugriff bei der Datenübertragung zwischen entfernten Sendern und Empfängern, sondern beispielsweise auch bei der Datenverarbeitung innerhalb eines Systems, bei dem der unberechtigte Zugriff zu Daten verhindert werden soll.

Aus der DE-AS 1237366 ist ein Verfahren bekannt, das den Anfangszustand eines Schlüsseltextgenerators in Abhängigkeit vom Ergebnis der Mischung einer ersten mit einer zweiten Zustandsinformation einstellt, wobei die erste Zustandsinformation sendeseitig vorzugsweise mittels eines Zufallsgenerators erzeugt und unverschlüsselt an die Empfangsseite übertragen wird.

Dieses Verfahren hat den Nachteil, daß das Gesetz für das Bilden der Binärzeichenfolge des Schlüsseltextes durch den starren Schaltungsaufbau des Schlüsseltextgenerators festgelegt ist und durch Ändern der Anfangsstellung nur ein anderer Abschnitt aus der Gesamtschlüsseltextfolge als neuer Schlüsseltext ausgewählt werden kann. Außerdem muß für jede Einstellung mittels eines Zufallsgenerators ein neuer Zusatzschlüssel erzeugt werden.

Aus der DE-OS 2457027 ist ein Verfahren zum Einstellen eines Schlüsseltextgenerators bekannt, bei dem ein Grundschlüsselwort bestimmend ist für die Anfangsstellung des Schlüsseltextgenerators und ein Zusatzschlüssel in Verbindung mit dem Grundschlüsselwort das Bildungsgesetz für die Binärzeichenfolge des Schlüsseltextes erstellt.

Dieses Verfahren arbeitet zwar nicht mehr mit einem starren Bildungsgesetz für die Binärzeichenfolge des Schlüsseltextes und ist damit wesentlich sicherer gegen unbefugtes Entschlüsseln, aber es wäre viel zu aufwendig, wenn es bei gleicher Sicherheit auch rundspruchfähig gemacht werden sollte, d. h., wenn in kurzen Zeitabständen immer wieder neue Zusatzschlüssel erzeugt, übertragen und eingestellt werden müßten.

Die zu der Erfindung führende Aufgabe war es, ein Verfahren anzugeben, das bei größtmöglicher Sicherheit Rundspruchfähigkeit erlaubt und mit geringem Aufwand verwirklicht werden kann.

Die Aufgabe wird gelöst, wie im Anspruch 1 beschrieben.

Die Fig. 1 zeigt den prinzipiellen Aufbau von Schlüsselgeräten,

die Fig. 2 den Durchlaufbetrieb des sendeseitigen Schlüsseltextgenerators.

Die Fig. 3 zeigt die verschlüsselte Übertragung der Registerstände zur identischen Einstellung der Schlüsseltextgeneratoren auf der Sende- und Empfangsseite.

Anhand der Figuren sei im folgenden ein Ausführungsbeispiel für die Verwirklichung des Verfahrens näher beschrieben.

Nach Fig. 1 bestehen die Schlüsseltextgeneratoren aus einer Anzahl von Schlüsseltextbildungsregistern $A1$ bis An, z. B. aus rückgekoppelten Schieberegistern, deren Rückkopplungsnetzwerke programmierbar sind; weiterhin aus einem Zuordner-Schaltnetzwerk C, das die Verknüpfungen der Register untereinander einstellt; ferner aus einem Bildungsgesetzregister B mit einer Speicherkapazität von n Bit, so daß eine Einstellvielfalt von 2^n verschiedenen Bildungsgesetzen möglich ist.

Die prinzipielle Arbeitsweise einer Datenverschlüsselung ist folgende:

Sendeseitig wird ein Klartext KT mit Hilfe eines Verknüpfungsgliedes mit dem Schlüsseltext ST verknüpft, so daß sich der Geheimtext GT ergibt, der übertragen wird. Empfangsseitig wird aus dem Geheimtext GT durch Verknüpfung mit dem nach identischen Regeln gewonnenen Schlüsseltext ST der Klartext wieder zurückgewonnen.

Im Durchlaufbetrieb des Schlüsseltextgenerators nach Fig. 2 wird die Ausgangsstellung der Schlüsseltextgeneratoren erwürfelt, von der aus am Sender verschlüsselt und am Empfänger entschlüsselt wird. Nach Anlegen der Betriebsspannung nehmen die Schlüsseltextbildungsregister A und das Bildungsgesetzregister B eine unbestimmte Anfangsstellung ein, die durch den Durchlaufbetrieb noch verändert wird. Während des Durchlaufbetriebes wird ein frei laufender Takt $T1$ aus einem astabilen Multivibrator oder einem Zufallsgenerator angelegt, der asynchron zum Übertragungsschrittakt die Schlüsseltextbildungsregister A um eine unbestimmte Anzahl von Durchlauftakten weiterschaltet. Der Schlüsseltextgenerator arbeitet dabei zunächst mit einem im Bildungsgesetzregister B gespeicherten unbestimmten Bildungsgesetz, welches während des Durchlaufbetriebes noch laufend dadurch verändert wird, daß die durch das Zuordner-Schaltwerk C verknüpfte Bitfolge durch das Bildungsgesetzregister B hindurchgeschoben wird.

In einer Varianten des Durchlaufbetriebes nach Anspruch 7 wird in den Kreislauf, beispielsweise zwischen dem Ausgang des Zuordnungsnetzwerkes C und dem Eingang des Bildungsgesetzregisters B, zusätzlich ein Zufallsgenerator eingeschaltet, der den Würfelvorgang steuert.

Der freilaufende Durchlaufbetrieb wird eine gewisse Mindestzeit durchgeführt, nach der diese Arbeitsweise zu jedem beliebigen Zeitpunkt durch Stillsetzen des Taktes $T1$ abgebrochen werden kann. Zum Zeitpunkt »Durchlaufbetrieb-Ende« haben dann alle Registerelemente des Schlüsseltextgenerators eine zufällige Ausgangsstellung, d. h. es wurde ein zufälliges Bildungsgesetz und eine zufällige Startposition des Schlüsseltextgenerators »erwürfelt«.

Zum Aufbau einer verschlüsselten Nachrichtenverbindung zwischen einem Sender und einem oder mehreren Empfängern, muß den Empfängern das Bildungsgesetz und die Ausgangsstellung des Schlüsseltextgenerators mitgeteilt werden.

In einem Ausführungsbeispiel nach Fig. 3 werden dazu sendeseitig die Schlüsseltextbildungsregister A und Bildungsgesetzregister B hintereinander geschaltet, seriell ausgelesen und empfangsseitig eingelesen, so daß nach y Übertragungsschrittakten sende- und empfangsseitig an allen Registerstellen vom Schlüsseltextbildungsregister A und vom Bildungsgesetzregister B eine übereinstimmende Ausgangsstellung herrscht.

Bei verschlüsselter Nachrichtenübertragung sollen nur solche Teilnehmer eine Entschlüsselung durchführen können, die dazu mit dem Grundschlüssel autorisiert werden. Deshalb muß die Übertragung der Registerstände des sendeseitigen Schlüsseltextgenerators zu den Empfängern verschlüsselt erfolgen. Die Verschlüsselung kann beispielsweise durch linear rückgekoppelte Schieberegister $SC1$ und $SC2$, die

auch als »Scramler« bekannt sind, erfolgen.

Diese Schieberegister sind auf der Sendeseite und auf der Empfangsseite identisch aufgebaut, und ihre Voreinstellung wird durch einen zwischen den korrespondierenden Teilnehmern abgestimmten Grundschlüssel *GS* festgelegt.

Ein weiteres Ausführungsbeispiel nach Anspruch 3 arbeitet in folgender Weise:

Die durch den Durchlaufbetrieb »erwürfelte« Anfangsstellung des Schlüsseltextgenerators wird in einen Zwischenspeicher *ZS*1 (nicht dargestellt) gespeichert. Danach werden einzelne oder alle Schlüsseltextbildungsregister *A* und/oder das Bildungsgesetzregister *B* sende- und empfangsseitig vom Grundschlüssel *GS* eingestellt. Zur verschlüsselten Übertragung der Anfangsstellung des Schlüsseltextgenerators wird dem Verknüpfungsglied (Fig. 1) die im Zwischenspeicher *ZS*1 gespeicherte Anfangsstellung als Klartext *KT* und der vom Grundschlüssel *GS* festgelegte Schlüsseltext *SO* des Schlüsseltextgenerators zugeführt. Die als Geheimtext *GT* übertragene Anfangsstellung wird auf der Empfangsseite als Klartext *KT* wiedergewonnen und in einem Zwischenspeicher *ZS*2 (nicht dargestellt) gespeichert. Vor der eigentlichen Nachrichtenübertragung wird nun sende- und empfangsseitig die Anfangsstellung aus den Zwischenspeichern *ZS*1 bzw. *ZS*2 in den Schlüsseltextgenerator eingeschoben.

Während der verschlüsselten Nachrichtenübertragung werden die Schlüsseltextbildungsregister *A* sende- und empfangsseitig synchron weitergeschaltet, dagegen bleiben die Registerstände des Bildungsgesetzregisters *B* bis zu einer neuen Einstellung der Ausgangsstellung fest bestehen.

Bei einmaliger Synchronisierung vor einer verschlüsselten Nachrichtenübertragung wird sendeseitig das Bildungsgesetz und die Ausgangsstellung des Schlüsseltextgenerators erwürfelt und den Empfängern übertragen.

In einem Ausführungsbeispiel nach Anspruch 6 wird das Bildungsgesetz des Schlüsseltextgenerators auf der Sende- und Empfangsseite errechnet, so daß eine verschlüsselte Übertragung des Bildungsgesetzes entfällt. Das Bildungsgesetz wird aufgrund der Anfangsstellung der Schlüsseltextbildungsregister *A*1 bis *An* nach einer vereinbarten Vorschrift im Schlüsseltextgenerator berechnet und sende- und empfangsseitig in einem Zwischenspeicher *ZS*3 bzw. *ZS*4 (nicht dargestellt) gespeichert. Vor der eigentlichen Nachrichtenver- bzw. -entschlüsselung wird das Bildungsgesetz aus den Zwischenspeichern *ZS*3 bzw. *ZS*4 in die jeweiligen Bildungsgesetzregister *B* des Schlüsseltextgenerators übernommen.

Dagegen wird bei sich wiederholender Synchronisierung, wie dies bei Rundspruchbetrieb notwendig ist, vom Sender zu festgelegten Zeitpunkten immer wieder sein aktueller Registerstand im Schlüsseltextbildungsregister *A* und gegebenenfalls sein neues oder gleichbleibendes Bildungsgesetz im Bildungsgesetzregister *B* übertragen. Neu hinzukommende Empfänger haben dann Gelegenheit, sich in laufende Übermittlungen einzuphasen. Dazu muß der Schlüsseltextgenerator nur jeweils um *y* Takte den normalen Nachrichtenfluß unterbrechen.

Hierzu 2 Blatt Zeichnungen

Nummer: 27 08 421
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: 29. Juni 1978

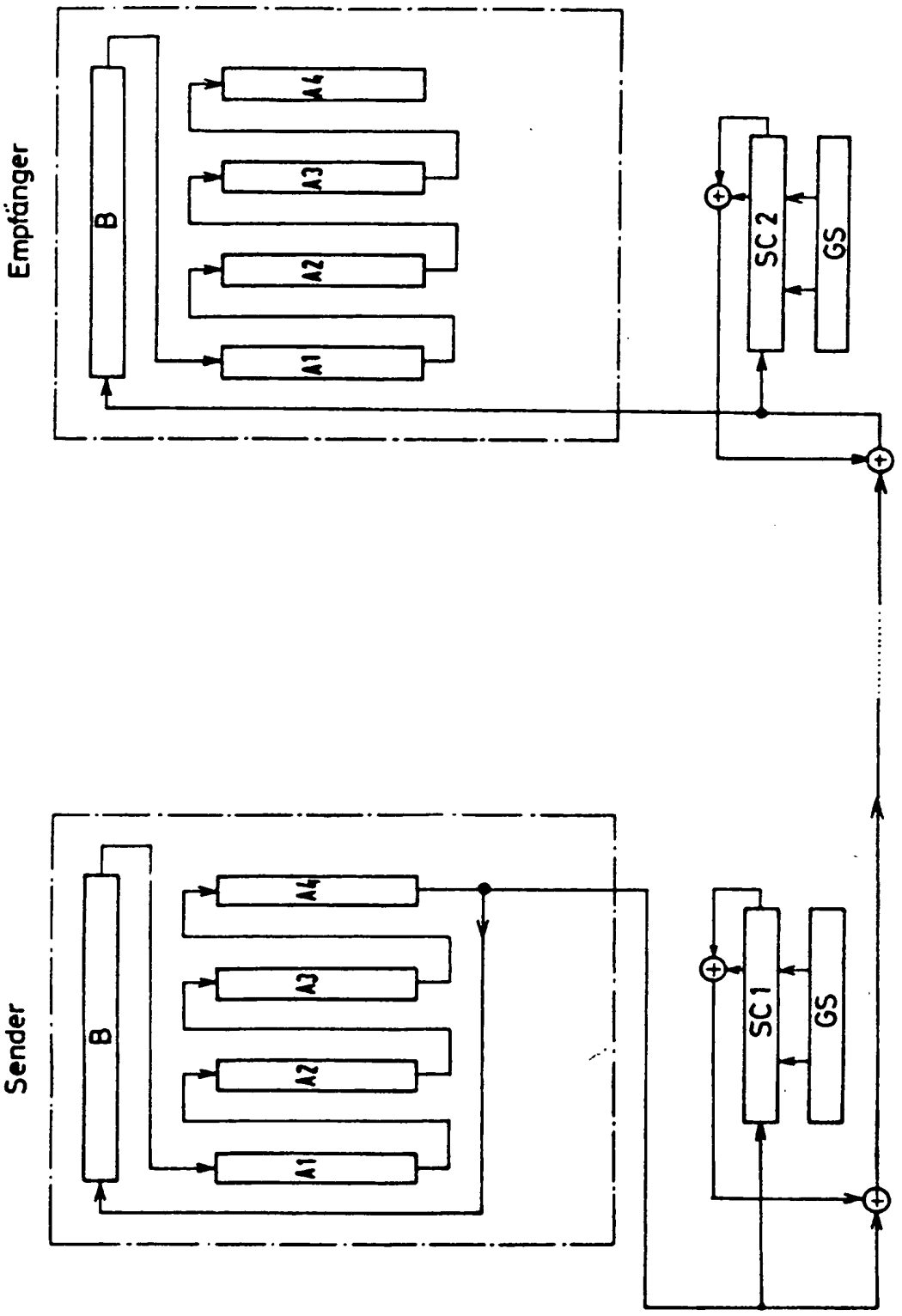

Fig. 3

Nummer: 27 06 421
Int. Cl.²: H 04 L 9/02
Bekanntmachungstag: 29. Juni 1978

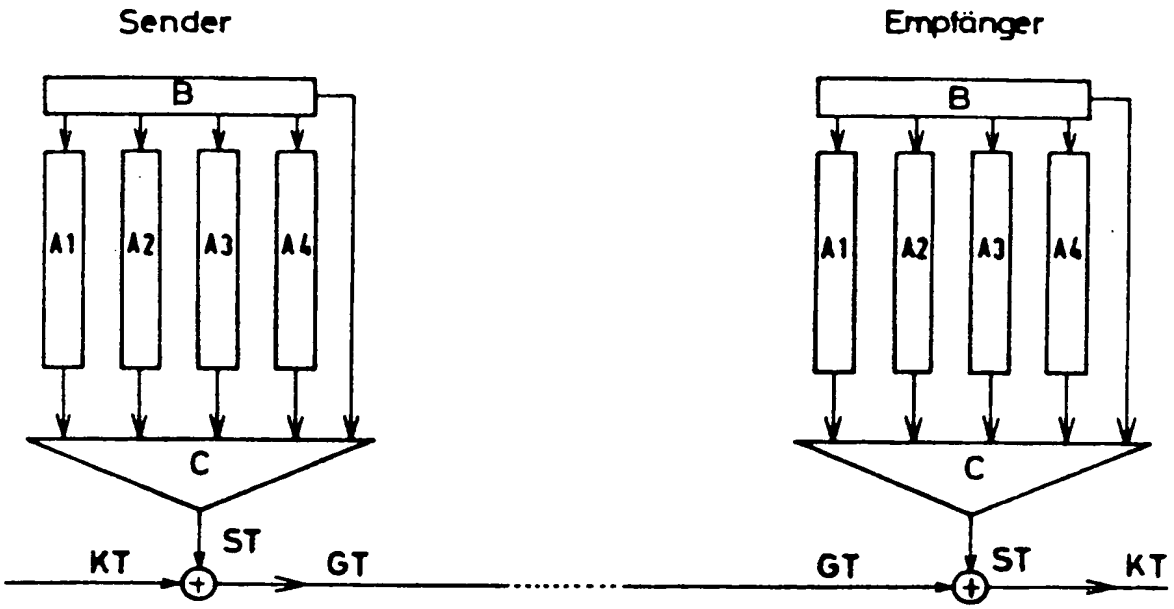

Fig. 1

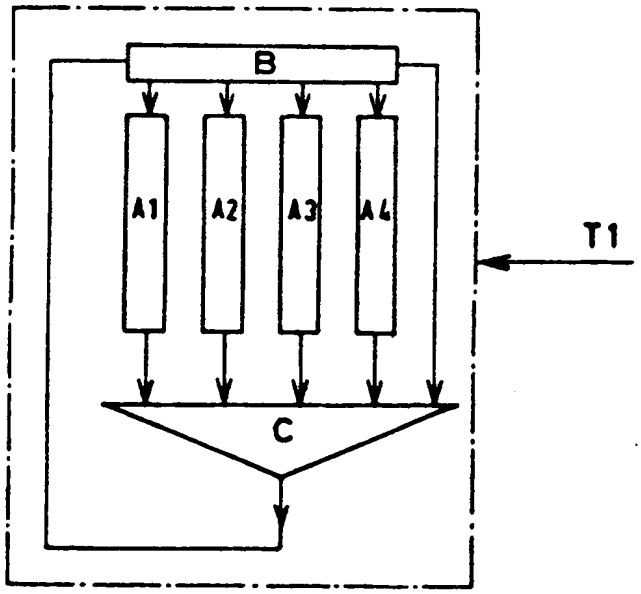

Fig. 2